Notice of References Cited	Application/Control No. 09/877,655	Applicant(s)/Patent Under Reexamination SHACHAM ET AL.	
	Examiner Michael J Simitoski	Art Unit 2134	Page 1 of 4

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-5,848,159	12-1998	Collins et al.	380/30
	B	US-6,578,061	06-2003	Aoki et al.	708/520
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Boneh, Dan et al. "An Attack on RSA Given a Small Fraction of the Private Key Bits", 1998.
	V	Boneh, Dan et al. "Cryptanalysis of RSA with Private Key d Less Than N^0.292 (extended abstract)", May 1999.
	W	Boneh, Dan et al. "Efficient Generation of Shared RSA Keys (extended abstract)".
	X	Boneh, Dan. "Twenty Years of Attacks on the RSA Cryptosystem", February 1999.

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited

Application/Control No. 09/877,655	Applicant(s)/Patent Under Reexamination SHACHAM ET AL.	
Examiner Michael J Simitoski	Art Unit 2134	Page 2 of 4

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Durfee, Glenn et al. "Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99", 2000.
	V	Fiat, Amos. "Batch RSA", 1998.
	W	Grobschadl, Johann. "The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip", December 2000.
	X	Immerman, Neil. "Homework 4 with Extensive Hints", March 2000.

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 09/877,655	Applicant(s)/Patent Under Reexamination SHACHAM ET AL.	
	Examiner Michael J Simitoski	Art Unit 2134	Page 3 of 4

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Menezes, Alfred J. et al. Handbook of Applied Cryptography, 1996 CRC Press, pp. §8.2-8.3 & §14.5.
	V	Oppliger, Rolf. "Authoriation Methods for E-Commerce Applications".
	W	RSA. "PKCS #1 v2.0 Amendment 1: Multi-Prime RSA", May 2000.
	X	Shand, M. et al. "Fast Implementations of RSA Cryptography", 1993.

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 09/877,655	Applicant(s)/Patent Under Reexamination SHACHAM ET AL.	
	Examiner Michael J Simitoski	Art Unit 2134	Page 4 of 4

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Stallings, William. Network Security Essentials: Applications and Standards", Prentice-Hall, November 1999.
	V	Takagi, Tsuyoshi. "Fast RSA-Type Cryptosystem modulo p^kq", 1998.
	W	Takagi, Tsuyoshi. "Fast RSA-Type Cryptosystems Using N-Adic Expansion", 1997.
	X	Wiener, Michael J. "Cryptanalysis of Short RSA Secret Exponents", 1989.

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.